PTO P543 Chinese Article

Po

Visional Secret Sharing Technology
[Shijueshi Mimi Fenxiang Jishu]

Po Hsisong, Yang Chinglung

NOTICE: BECAUSE OF COPYRIGHT RESTRICTION THIS TRANSLATION IS FOR THE INTERNAL USE OF PTO PERSONNEL AND ANY REFERENCE TO THIS PAPER MUST BE TO THE ORIGINAL

FOREIGN SOURCE.

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C.

October 2004

Translated by: Schreiber Translations, Inc.

<u>Translated Title</u>: Visional Secret Sharing Technology

Foreign Title : Shijueshi Mimi Fenxiang Jishu

Authors : Po Hsisong, Yang Chinglung

Author Affiliation : Department of Electrics, National

Chengkung University

<u>Source</u>: Patent Gazette of Republic of China

## Visional Secret Sharing Technology Shijueshi Mimi Fenxiang Jishu

Po Hsisong, Yang Chinglung

[57] Scope of Patent in Application
This patent concerns:

1. A (k,n) visional secret sharing method that can detect errors and counterfeit transparencies, wherein k, n are positive integrals. The method includes:

Providing  $n \times m$  shared matrixes Sw and Sb representing white and black pixels in the (k,n) visional secret sharing method;

Expanding the  $n \times m$  shared matrixes Sw and Sb into four  $(n+1)\times (m+2)$  shared matrixes Sww, Swb, Sbw, and Sbb:

$$Sww = \begin{bmatrix} \frac{10}{10} & 0 & \cdots & 0 \\ \vdots & Sw & \vdots & Sw \\ 10 & & & \end{bmatrix}$$

$$Swb = \begin{bmatrix} \frac{10}{10} & 0 & \cdots & 0 \\ 10 & & & \vdots & Sb \\ 10 & & & \end{bmatrix}$$

 $<sup>^{\</sup>mbox{\scriptsize 1}}$  Numbers in the margin indicate pagination in the foreign text.

$$Sbw = \begin{bmatrix} 10 & 0 & \cdots & 0 \\ 10 & & & \\ \vdots & Sw & & \\ 10 & & & \end{bmatrix} \qquad Sbb = \begin{bmatrix} 10 & 0 & \cdots & 0 \\ 10 & & & \\ \vdots & Sb & & \\ 10 & & & \end{bmatrix}, \text{ and}$$

based on the four  $(n+1)\times(m+2)$  shared matrixes Sww, Swb, Sbw, Sbb, dividing a secret image comprised of multiple pixels into n+1 sheets of transparency, whereas each pixel in the secret image corresponds to m-2 small pixels, whereas shared matrix Sww is applied when the pixels in the secret image and in an examining image are all white, whereas shared matrix Swb is applied when the pixels in the secret image are white and the pixels in the examining image are black, whereas shared matrix Sbw is applied when the pixels in the secret image are black and the pixels in the examining image are white, whereas shared matrix Sbb is applied when the pixels in the secret image and in an examining image are all black;

As a result, the formed  $1^{st}$  transparency can be used for detecting errors and counterfeit transparencies. The examining image can be obtained from superimposition of the first transparency with other transparences. The secret image can be obtained from superimposition of any k sheets of transparency from other n transparencies.

2. A (k,n) visional secret sharing method that can detect errors and counterfeit transparencies, wherein k, n are positive integrals, and  $k \geq 3$ . The method includes:

Providing  $n \times m$  shared matrixes Sw and Sb representing white and black pixels in the (k,n) visional secret sharing method;

<u> /544</u>

Expanding the  $n \times m$  shared matrixes Sw and Sb into four  $n \times [m+n \times (n-1)]$  shared matrixes Sww, Swb, Sbw, and Sbb:

$$Sww = \begin{bmatrix} 1010 \cdots 11 \\ 1011 \cdots \vdots \\ 1010 \cdots \vdots \\ \vdots 11 \cdots 11 \\ \vdots \vdots \cdots 10 \\ 1111 \cdots 10 \end{bmatrix} Sw$$

$$Swb = \begin{bmatrix} 1010 \cdots 11 \\ 1010 \cdots \vdots \\ \vdots 11 \cdots 11 \\ \vdots \vdots \cdots 10 \\ 1111 \cdots \vdots \end{bmatrix} Sw$$

$$Sbw = \begin{bmatrix} 1010 \cdots 11 \\ 0111 \cdots \vdots \\ 1001 \cdots \vdots \\ \vdots 11 \cdots 11 \\ \vdots \vdots \cdots 10 \\ 1111 \cdots 01 \end{bmatrix} Sw$$

$$Sbb = \begin{bmatrix} 1010 \cdots 11 \\ 0111 \cdots \vdots \\ 1001 \cdots \vdots \\ \vdots 11 \cdots 11 \\ \vdots \vdots \cdots 10 \\ 1111 \cdots 01 \end{bmatrix} Sb$$

based on the four  $n \times [m+n \times (n-1)]$  shared matrixes Sww, Swb, Sbw, Sbb, dividing a secret image comprised of multiple pixels

into n sheets of transparency, whereas each pixel in the secret image corresponds to  $m+n\times(n-1)$  small pixels, whereas shared matrix Sww is applied when the pixels in the secret image and in an examining image are all white, whereas shared matrix Swb is applied when the pixels in the secret image are white and the pixels in the examining image are black, whereas shared matrix Sbw is applied when the pixels in the secret image are black and the pixels in the examining image are white, whereas shared matrix Sbb is applied when the pixels in the secret image and in an examining image are all black;

As a result, the superimposition of any two transparencies from the above-mentioned n transparencies can be used for detecting errors and counterfeit transparencies, and obtaining the examining image. The secret image can be obtained from superimposition of any k sheets of transparency from other n transparencies.

3. A  $(1 \rightarrow n)$  visional secret sharing method that can sequentially shared n-1 sheets of secret images, detect errors and counterfeit transparencies, wherein k, n are positive integrals, and  $k \geq 3$ . The method includes:

Providing  $u \times 2^{u-1}$  shared matrixes Sw and Sb representing white and black pixels in the (u,u) visional secret sharing method;

Assuming the  $u \times 2^{u-1}$  shared matrixes  $Sw^{(l-1)}$  and  $Sb^{(l-1)}$  as [0] and [1], and obtaining  $2^u$  shared matrixes in regression manner;

$$S_{ww}^{(1\to u+1)} = \begin{bmatrix} S_{w}^{(u+1,u-1)} & 1 & \cdots & \\ S_{w}^{(1\to u+1)} & S_{wb}^{(1\to u+1)} & \cdots & \\ S_{bw}^{(1\to u+1)} & S_{bb}^{(1\to u+1)} & \cdots & \\ S_{bw}^{(1\to u+1)} & S_{bb}^{(1\to u+1)} & \cdots & \\ S_{b}^{(1\to u+1)$$

n sheets of transparencies can be obtained through

transformation of the  $2^u$  shared matrixes, whereas shared matrix Sww is applied when the pixels in the first secret image are white and the pixels in the second secret image are white....., whereas shared matrix Swb is applied when the pixels in the first secret image are white and the pixels in the second secret image are black....., whereas shared matrix Sbw is applied when the pixels in the first secret image are black and the pixels in the second secret image are white....., whereas shared matrix Sbb is applied when the pixels in the first secret image are black and the pixels in the second secret image are black and the pixels in the second secret image are black..., and so on.

As a result, the first secret image can be obtained through superimposition of the  $1^{\rm st}\sim 2^{\rm nd}$  transparencies, the second secret image can be obtained through superimposition of the  $1^{\rm st}\sim 3^{\rm rd}$  transparencies, and so on.

4. A color (k,k) visional secret sharing method that can conduct secret sharing to c-color secret images, wherein k is positive integral. The method includes:

Providing  $k \times 2^{k-1}$  shared matrixes  $B_0$  and  $B_1$  representing white pixels and black pixels in the black-white (k,k) visional secret sharing method, wherein the numbers of "l" in each column element are all even and odd numbers;

Extending the shared matrixes  $B_0$  and  $B_1$  to c number of  $k \times (c \times 2^{k-1})$  shared matrixes  $C_i$ :

(translator's note: formula not legible)

Based on the c number of  $k \times (c \times 2^{k-1})$  shared matrixes, transforming a color secret image comprised of multiple pixels into k number of transparencies. In this secret image, each pixel corresponds to  $c \times (2^{k-1})$  number of small pixels. Shared matrix  $C_0$  is applied when the pixels of the color secret image are color 0 pixels; Shared matrix  $C_1$  is applied when the pixels of the color secret image are color 1 pixels....., and so on.

As a result, the color secret image can be obtained from superimposition of  $\boldsymbol{k}$  sheets of transparencies.

/545

5. A color (k,n) visional secret sharing method that can conduct secret sharing to c-color secret images, wherein k and n are positive integrals. The method includes:

Providing  $n \times m$  shared matrixes  $B_0$  and  $B_1$  representing white pixels and black pixels in the black-white (k,n) visional secret sharing method;

Extending the shared matrixes  $B_0$  and  $B_1$  to c number of  $n \times (c \times m)$  shared matrixes  $C_i$ :

(translator's note: formula not legible)

Based on the c number of  $n \times (c \times m)$  shared matrixes, transforming a color secret image comprised of multiple pixels into n number of transparencies. In this secret image, each pixel corresponds to  $c \times m$  number of small pixels. Shared matrix  $C_0$  is applied when the pixels of the color secret image are color 0 pixels; Shared matrix  $C_1$  is applied when the pixels of the color secret image are color 1 pixels....., and so on.

As a result, the color secret image can be obtained from superimposition of any k sheets of transparencies from the above-mentioned k transparencies.

- 6. A visional secret sharing method as described in Claims 1, 2, 3, 4, or 5, whereas the transparencies can be stored and superimposed by a computer image editing software.
- 7. A visional secret sharing method as described in Claim 6, whereas the transparencies can be put in both the host and client computers of a network system for identifying purpose and preventing illegal users to enter the system.
- 8. A visional secret sharing method as described in Claim 6, whereas the transparencies can be made into a goggles to be placed in front of the computer screen.
- 9. A visional secret sharing method as described in Claim 6, whereas the transparencies can be made into a thin film to cover on the LCD of a mobile phone set.
- 10. A visional secret sharing method as described in Claim 4, the columns having "\*" (representing black color) in the whole column in the shared matrix  $C_i$  can be deleted so as to further reduce the shared length b to:

 $b = c \times 2^{k-1} - 1 \quad \text{(when $c$ is an even number), and}$   $b = c \times 2_{k-1} - c + 1 \quad \text{(when $c$ is an odd number).}$ 

Brief Explanations to Drawings:

Fig. 1A ~ Fig. 1C are illustrations of application of the known visional secret sharing technology in the Internet;

Fig. 2 is an illustration of application of the known visional secret sharing technology in mobile phones;

Fig. 3 is an illustration of the known (k,n) visional secret sharing technology;

Fig. 4A is an image (the first secret image) obtained through superimposition of the 1<sup>st</sup> shared image with other shared images as described in Implementation 1 of this invention;

Fig. 4B is an image (the second secret image) obtained through superimposition of any two shared images from the  $2^{nd}$ ,  $3^{rd}$ ,  $4^{th}$ , and  $5^{th}$  shared images as described in Implementation 1 of this invention;

Fig. 5A is an illustration of the 1<sup>st</sup> shared image as described in Implementation 3 of this invention;

Fig. 5B is an illustration of the image (the first secret image) obtained through superimposition of the  $1^{\rm st}$  shared image and the  $2^{\rm nd}$  shared image as described in Implementation 3 of this invention;

Fig. 5C is an illustration of the image (the second secret image) obtained through superimposition of the 1st shared image,

the  $2^{nd}$  shared image, and the  $3^{rd}$  shared image as described in Implementation 3 of this invention;

Fig. 6A and Fig. 6B are illustrations of pixels in known color VSS technology;

Fig. 7A and Fig. 7B are illustrations of pixels in color VSS technology as described in Implementation 4 of this invention;

Fig. 8A is an illustration of colors of single shared image as described in Implementation 4 of this invention;

Fig. 8B is an illustration of colors of the image after superimposition of any two shared images as described in Implementation 4 of this invention;

Fig. 8C is an illustration of colors of the image after superimposition of any three shared images as described in Implementation 4 of this invention;

Fig. 9A ~ Fig. 9D are comparisons in computer expression between the color VSS technology in this invention and the known color VSS technology.

/546

\*\*\*\*\*

\*\*\*\*

Fig. 1A

\*\*\*\*\*

\*\*\*\*

Fig. 1B

\*\*\*\*

\*\*\*\*

Fig. 1C

<u>/547</u>

\*\*\*\*

\*\*\*\*

Fig. 2

\*\*\*\*\*

\*\*\*\*\*

Fig. 3

<u>/548</u>

. . . . . .

\*\*\*\*

Fig. 4A

\*\*\*\*

\*\*\*\*\*

Fig. 4B

\*\*\*\*\*

\*\*\*\*\*

Fig. 5A

\*\*\*\*\*

\*\*\*\*\*

Fig. 5B

\*\*\*\*\*

\*\*\*\*\*

<u>/549</u>

Fig. 5C

\*\*\*\*\*

\*\*\*\*\*

Fig. 6A

\*\*\*\*

\*\*\*\*\*

Fig. 6B

<u>/550</u>

\*\*\*\*\*

\*\*\*\*\*

Fig. 7A

\*\*\*\*

\*\*\*\*

Fig. 7B

\*\*\*\*\*

\*\*\*\*

Fig. 8A

\*\*\*\*\*

\*\*\*\*

Fig. 8B

#### 中華民國專利公報(19)(12)

ミロリ公告編輯:364957

[編]中華民國88年(1999)07月21日

登 明

全 10 頁

[5]] n t · C | 6:G06F11/00 G09C1/00

(54)名

荷:促促式秘密分享技術

(21)申請案 號:87102660

(22)中萬日間:中華民國87年(1998)02月24日

(72) 登 明 人:

相演派 傷度疫 台南市大學路一號(圖立成功大學電機系)

海塘市自由二路六卷五十七颗

(71)中 請 人: 相演任

古南市大學路一號(圖立成功大學電觀系)

[四]化 理 人:洪澄文 先生

1

#### [57]申請專利範圍:

1.一種可偵測錯誤及偽造投影片之(k,n) 視覺式秘密分享方法,其中,k,n為 正整數,包括:

提供一(k,n)觀覺式秘密分享方法中表 示白色及黑色像素之n×m分享矩陣Sw 及 Sb:

將該些n×m分享矩陣Sw及Sb擴展為 四個(n+1)×(m+2)分享矩陣Sww・ Swb・Sbw及Sbb;以及

$$Sww = \begin{bmatrix} 100 \cdots 0 \\ 10 \\ \vdots \\ Sw \\ 10 \end{bmatrix} \qquad Swb = \begin{bmatrix} 100 \cdots 0 \\ 10 \\ \vdots \\ Sb \\ 10 \end{bmatrix}$$

$$Sbw = \begin{bmatrix} 100 \cdots 0 \\ 10 \\ \vdots \\ Sb \\ 10 \end{bmatrix}$$

$$Sbw = \begin{bmatrix} 100 \cdots 0 \\ 10 \\ \vdots \\ Sb \\ 10 \end{bmatrix}$$

根據該四個(n + 1)×(m + 2)分享矩陣 Sww·Swb·Sbw及Sbb將一由複數像 紊組成之秘密影像分成n+1張投影片 且該秘密影像中各像素係對應m-2個 小像素,其中,分享矩陣 Sww 在該秘密影像及一檢查影像之像素均為白色時使用,分享矩陣 Swb 在該秘密影像之像素為白色且該檢查影像之像素為黑色 5. 時使用,分享矩陣 Sbw 在該秘密影像之像素為黑色且該檢查影像之像素為白色時使用,而分享矩陣 Sbb 則在該秘密影像及該檢查影像之像素均為黑色時使用:

2

10. 是以,形成之第1强投影片可做為偵測 錯誤及偽造投影片之用,其與各別投影 片重疊可得該檢查影像,而其他n强投 影片中任k强投影片重疊則可得到該秘 密影像。

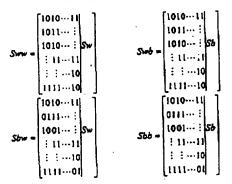
5.

10.

15.

3

將該些 n × m 分享矩陣 Sw 及 Sb 擴展為 四個 n × [m + n × (n-1)]分享矩陣 Sww、 Swb 、 Sbw 及 Sbb: 以及



根據該四個n×[m+n×(n-1)]分享矩陣 Sww、Swb、Sbb X Sbb X Sbb X - 由複數像 素組成之秘密影像分成n張投影片且該 秘密影像中各像素係對應m+n×(n-1) 個小像素,其中,分享矩陣 Sww 在該 秘密影像及一檢查影像之像素均為自色時使用,分享矩陣 Swb 在該秘密影像之像素為自色且該檢查影像之像素為黑色且數檢查影像之像素為 自色時使用,而分享矩陣 Sbb 則在該秘密影像之像素為黑色且數檢查影像之像素均為黑色時使用;

是以,上述n張投影片中任兩張投影片 重量可用以偵測錯誤及偽造之投影片並 得到該檢查影像,而上述n張投影片中 任 k 張投影片重疊則可得到該秘密影 像。

3.一種(1→n)視覺式秘密分享方法,可依 序分享n-1 張秘密影像,其中,k,n為 正整數,包括:

將該些 u × 2<sup>n-1</sup> 分享矩陣 Sw<sup>(1-1)</sup>及 Sb<sup>(1</sup> -1<sup>1</sup>, 設為[0]及[1], 並以遞迴方式得到 2<sup>n</sup>個分享矩陣:

$$S_{(1-n+1)}^{(1-n+1)} = \begin{bmatrix} S_{(n+1^{n+1})}^{(n+1)} & & & & \\ S_{(1-n)}^{(n+1)} & & & \\ & & &$$

根據該2"個分享矩陣轉換以得到n張投影片,其中,分享矩陣Sww...在一第一秘密影像之像素為白色,一第二秘密影像之像素為白色,...時使用,分享矩陣Swb...在該第一秘密影像之像素為黑色,...時使用,分享矩陣Sbw...在該第一秘密影像之像素為黑色,...時使用,分享矩陣Sbw...在該第一秘密影像之像素為白色,...時使用,分享矩陣Sbb...在該第一秘密影像為黑色,該第二秘密影像之像素為白色,...時使用,分享矩陣Sbb...在該第一秘密影像為黑色,...時使用,餘以此類推;

如此,第1~2張投影片重疊可得到該 第一秘密影像,第1~3張投影片重疊 可得到該第二秘密影像,餘以此類推。

- 20. 4.一種彩色(k,k)視覺式秘密分享方法,可對 c 色秘密影像進行秘密分享,其中,k為正整數,包括: 提供一黑白(k,k)視覺式秘密分享方法
- 中表示白色像素及黑色像素之 k × 2<sup>1-1</sup> 25. 分享矩阵B<sub>0</sub>及B<sub>1</sub>,其各欄元素中 \*1″

的數目均為偶數及奇數: 根據該些分享矩陣B<sub>0</sub>及B<sub>1</sub>延伸為c個k ×(c×2<sup>k-1</sup>)分享矩陣Ci,其中

30.

根據該c個k×(c×2<sup>k-1</sup>)分享矩陣將一1 由複數像素組成之彩色秘密影像轉換成 k張投影片且該秘密影像中各像素係對 應c×(2<sup>k-1</sup>)個小像素、其中,分享矩陣 C。在該彩色秘密影像之像素為第0顏色 時使用,分享矩陣C,在該彩色秘密影 像之像素為第1顏色時使用,…,餘以 此類推;

如此,當k强投影片重疊時便可得到該 彩色秘密影像。

40.

35.

15.

5

5.一種彩色(k,n) 視覺式秘密分享方法,可對 c 色秘密影像進行秘密分享,其中,n、k 為正整數,包括:提供一黑白(k,n) 視覺式秘密分享方法

提供一為日(K,n)病党式的留厅学方法 中表示白色像素及黑色像素之n×m分 享矩陣B<sub>o</sub>及B<sub>i</sub>;

根據該些分享矩陣  $B_c$   $D_c$   $D_c$ 

C, - for serie or full-month formation of fo

根據該c個n×(c×m)分享矩陣將一由 複數像素組成之彩色秘密影像轉換成n 張投影片且該秘密影像中各像素係對應 c×m個小像素,其中,分享矩陣C。在 該彩色秘密影像之像素為第0顏色時使 用,分享矩陣C,在該彩色秘密影像之 像素為第1顏色時使用,...,餘以此類 推:

如此,當上述n 張投影片中任何 k 張投影片重叠後便可以得到該彩色秘密影像。

- 6.如申請專利範圍第1、2、3、4或5項 所述之親覺式秘密分享方法,其中,該 些投影片亦可以電腦影像編輯軟體儲存 並且進行重疊成像的工作。
- 7.如申請專利範圖第6項所述之視覺式秘 密分享方法,其中,該些投影片可分別 置網路系統之主機端及客戶端,藉以進 行辨證並防止非法使用者進入。
- 8.如申請專利範圍第6項所述之視覺式秘密分享方法,其中,該些投影片可製成一種目鏡,置於電腦營幕前方。
- 9.如申請專利範圖第6項所述之視覺式秘密分享方法,其中、該些投影片可製成一薄膜,覆蓋於行動電話手機之液晶單示螢幕上。
- 10.如申請專利範圍第 4 項所述之彩色視 覺式秘密分享方法,其中,該些分享矩 陣 Ci 中具有整列 \*\* (表示黑色)之欄

6

位可予以刪除,進而使分享長度b進一 步縮小至

 $b = c \times 2^{b \cdot l} - l(當 c 為偶數)$ ,以及  $b = c \times 2_{b \cdot l} - c + 1(當 c 為奇數)$ 。

5. 圖式簡單說明:

第一圖A~第一圖C係習知視覺式秘密分享技術應用於網際網路之示意圖:

第二圖係習知視覺式秘密分享技術 應用於行動電話手機之示意圖:

10. 第三圖係蓄知(k · n)視覺式秘密分 享技術之示意圖:

第四圖A係本發明例1中第1張分享 — 影像與其他分享影像重疊所得之影像(即 第一秘密影像):

第四圖B係本發明例1中第2·3· 4·5張分享影像中任兩張分享影像重疊 後所得之影像(即第二秘密影像):

第五圖A係本發明例3中第1張分享 影像之示意圖:

20. 第五圖B係本發明例3中第1張分享 影像及第2張分享影像重量後所得結果 (第一秘密影像)之示意圖:

第五圖 C 係本發明例 3 中第 1 張分享 影像、第 2 張分享影像及第 3 張分享影像 25. 重量後所得結果(第二秘密影像)之示意 圖:

> 第六圖A及第六圖B係習知彩色VSS 技術中各像素之示意圖:

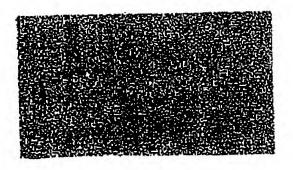
第七圖A及第七圖B係本發明實施例 30. 四中彩色 VSS 技術中各像素之示意圖:

第八圖A係本發明例4中單張分享影像之顏色示意圖:

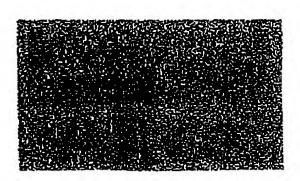
第八圖B係本發明例4中任兩張分享 影像重量後之顧色示意圖;

35. 第八圖C係本發明例4中三張分享影 像重疊後之顏色示意圖:以及

> 第九圖 A ~第九圖 D 係本發明彩色 VSS 技術與習知彩色 VSS 技術在電腦中 表示法之比較。



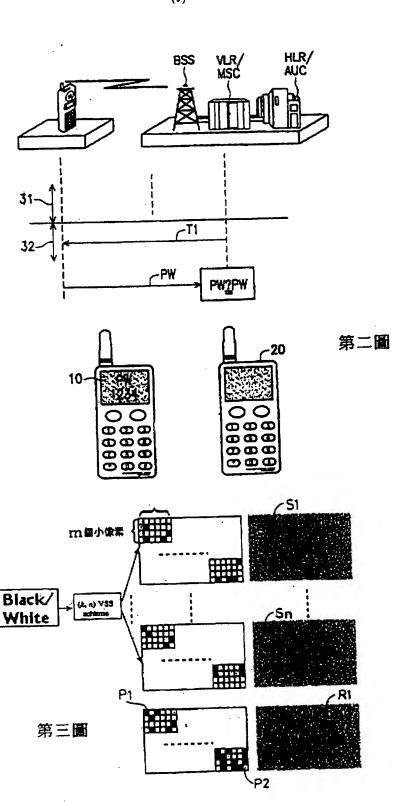
第一圖 A



第一圖 B

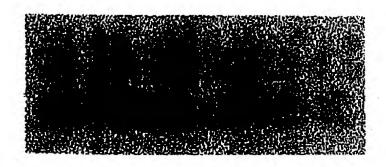


第一圖C

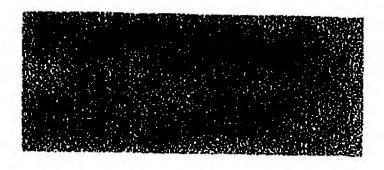




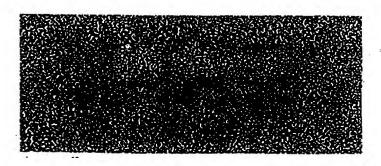
第四圖A



第四圖 B



第五圖A

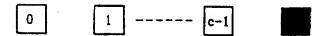


第五圖 B



第五圖C





### 第七圖A

## 第七圖 B



0 1 0 1 2

第八圖B

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:
☐ BLACK BORDERS
☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
☐ FADED TEXT OR DRAWING
☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
☐ SKEWED/SLANTED IMAGES
☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
☐ GRAY SCALE DOCUMENTS
☐ LÎNES OR MARKS ON ORIGINAL DOCUMENT
☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
OTHER:

# IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.